8/13/03

ProQuest

Help

Basic Search Advanced Search Topic Guide Marked List Language: English ▼

Databases selected: Multiple databases...

Article View

« Back to Results < Previous Article 7 of 18 Next > Publisher Information

Print Email □ Mark Article Abstract, Full Text, Page Image - PDF

Cookies on your hard drive

Wayland Hancock. American Agent & Broker. St. Louis: Jun 1997. Vol. 69, Iss. 6; pg. 8, 2 pgs

» Jump to full text

Subjects:	Web sites, Servers, Customer information f
Web sites, Servers, Customer information files, Privacy, Problems	
Classification Codes	9190 US, 5250 Telecommunications system
Locations:	US
Author(s):	Wayland Hancock
Publication title:	American Agent & Broker. St. Louis: Jun 19
Source Type:	Periodical
ISSN/ISBN:	00027200
ProQuest document ID:	12534355
Text Word Count	1128
Article URL:	http://gateway.proquest.com/openurl?ctx_ve

More Like This »Show Options for finding similar articles

Abstract (Article Summary)

When you disclose information about yourself to a commercial Web site, the site's server may store that identifying information on your hard drive in what is called a "cookie file." When you later visit the site, the site's server can access the cookie file and the information stored in it. Most Web site servers do not disclose that they use cookies. Web site servers argue that cookies are necessary for conducting accurate market research. Servers that monitor their Web site traffic claim that cookies allow them to distinguish between 50 site hits from 50 different people and 50 hits from one person. Your cookie file may contain a list of Web sites you have visited, online purchases you have made, or any other information about you.

Full Text (1128 words)

YOUR WEB browser may be storing cookies on your hard drive. I'm not referring to cookies of the chocolate-chip persuasion, but to ones that store lines of data containing personal information about you, your job and your interests.

When you disclose information about yourself to a commercial Web site, the site's server may store that identifying information on your hard drive in what's called a "cookie file." When you later visit that same Web site, the server can access the cookie file and the information stored in it.

Cookies were introduced about a year ago. However, most Web site servers do not disclose that they use them. In fact, most people who access the Web don't even realize they have cookie files on their hard drive. Using cookies raises an ethical question: Is it an invasion of privacy? Before answering that question, let's explain how cookie files are used, what their advantages and disadvantages are and what you can do about them.

Cookies are a mechanism that server-side connections can use to store and retrieve information from the client side of the connections. When you click on a Web site, your Web browser checks that link against your cookie file. If a compatible cookie exists for that link, the browser sends the cookie to the Web server along with your request for access to the site.

Web site servers argue that cookies are necessary for conducting accurate market research. Using cookies, they can distinguish between 50 site "hits" from 50 different people and 50 "hits" from one person. Servers who monitor their Web site traffic claim that cookies allow them to do this in a nondisruptive manner.

Your cookie file may contain a list of Web sites you have visited, online purchases you have made or any other information about you. Web site servers use the file to identify your interests and customize their services for you without having to ask you a lot of questions each time you visit their sites. Servers can use the cookies to identify specific clients who return to a site, even after an extended interval.

Shopping applications use "cookie technology" to store information about purchases. Sites supporting Web services can store the names of products that visitors buy and present information about only those products when visitors return to the sites. Newspapers with Web sites use data from your cookie to determine exactly who you are, where you live and what sections of the paper you regularly view.

Fee-based Internet service providers store registration information in cookies so users don't have to manually log on each time they access the service. They also can store user preferences. Netscape, for example, uses cookies to let users access its new personal workspace area and to store information about how users like their information presented. Microsoft offers similar features in its "start" page.

Web service providers are not supposed to be able to access cookies written for other providers. However, it's possible that a group of servers could agree to allow access to each other's cookies. Cookies are not executable programs and do not contain viruses. They can't read other information on your hard disk and can't give out your e-mail address without your permission. However, this doesn't mean that Web services are unable to send a virus, run an application or determine your e-mail address without your knowledge. There are programs out there that enable them to do this.)

Among the disadvantages of cookies is that some people worry about technology tracking their every move. Others worry about invasion of privacy because the cookies can transmit personal information. However, the only way cookies can do this is if you voluntarily give personal information to a Web site in the first place.

Legitimate arguments can be made for requiring Web site servers to disclose their use of cookies. For instance, users should be notified that their customer profiles will be taken before they browse a site. That the Web browser stores information on your hard drive certainly is a situation you should be warned about. Unfortunately, there are few privacy rules on the Internet, so you have to protect your own interests. A couple of suggestions can help you do that.

Locate your cookie file. The name and location of your cookie file depends upon your browser software. Netscape Navigator for Windows calls its file "cookie.txt" in the Netscape directory. Netscape Navigator for Macintosh stores cookies in a file called MagicCookie in the Netscape preferences folder. Internet Explorer stores cookies in a file called "emcookie.dat" in the Explorer directory.

Look at the contents of your cookie file. The file is not encrypted; you can open it with an ordinary text editor (like the "Write" program in Windows). The name of the Web server that gave you the cookie is the first word on every line of the file.

Options of what to do with your cookies range from completely destroying them to doing absolutely nothing. Your best course of action is to identify the Web sites that store cookies in your hard drive. Do this by enabling the "show alert before accepting a cookie" option on your browser. The option is on the Netscape 3 menu under "options, network preferences." With Internet Explorer, the option is in the advanced tab under "view options."

If you don't want any cookies stored on your computer, you can empty the contents of your cookie file, then mark the file "read only." In Windows, you can use the file manager to do this. Afterward, sites that attempt to write to the file will be unsuccessful. Still, this will not permanently rid you of cookies; they reside in memory whenever you spend time on a Web site.

You also can delete cookie files after each Web session. However, you must do this every time, because if a Web server finds no cookie file, it creates a new one. Remember that a Web site cannot set your particular preferences without this file.

I know of no way to program your computer to automatically accept cookies from certain sites and reject them from others, without installing a third-party program. Two programs that claim to give you more control over your browser's use of cookies are PGPcookie.cutter (http: //www/pgp.com) and Cookie Master (http://www.zd.net).

The World Wide Web has grown by leaps and bounds within the past few years, but there's still much uncharted territory. There are many benefits to performing transactions via the Internet. But because there are few regulatory standards, there exists great potential for fraudulent activities. Your best defense is to be cautious and look out for yourself. I guess that's just the way the cookie crumbles!

Correspondence may be addressed to Wayland "Buddy" Hancock, at his Internet E-mail address: Wayland.Hancock@bigfoot.com

^ Back to Top « Back to Results < Previous Article 7 of 18 Next > Publisher Information
Print Email □ Mark Article Abstract , Full Text , Page Image - PDF

Text-only interface